



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



010.102 Data/Media Security Policy

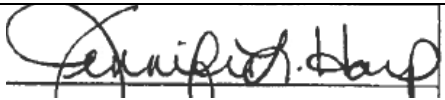

**Version 2.4
November 15, 2018**

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

Revision History

Date	Version	Description	Author
11/16/2006	1.0	Effective Date	CHFS OATS Policy Charter Team
11/15/2018	2.4	Review Date	CHFS OATS Policy Charter Team
11/15/2018	2.4	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	11/15/2018	Jennifer Harp	
CHFS Chief Information Security Officer (or designee)	11/15/2018	DENNIS E. LEBER	

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

Table of Contents

1	POLICY DEFINITIONS.....	4
2	POLICY OVERVIEW.....	6
2.1	PURPOSE	6
2.2	SCOPE	6
2.3	MANAGEMENT COMMITMENT.....	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES	6
2.5	COMPLIANCE	6
3	ROLES AND RESPONSIBILITIES	6
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO)	6
3.2	CHIEF PRIVACY OFFICER (CPO)	7
3.3	SECURITY/PRIVACY LEAD	7
3.4	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL	7
3.5	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
4	POLICY REQUIREMENTS	8
4.1	GENERAL	8
4.2	DATA CLASSIFICATION	8
4.3	EXTERNAL MARKINGS	8
4.4	EXTERNAL STORAGE DEVICE ACQUISITION AND PROCESS	8
4.5	REPRODUCTION.....	9
4.6	STORAGE AND SECURITY FOR NON-ELECTRONIC MEDIA	9
4.7	STORAGE AND SECURITY FOR ELECTRONIC MEDIA	9
4.8	DISPOSAL/DESTRUCTION FOR NON-ELECTRONIC MEDIA.....	10
4.9	DISPOSAL/DESTRUCTION FOR ELECTRONIC MEDIA	10
4.10	SHIPPING AND MANUAL HANDLING.....	10
4.11	FACSIMILE TRANSMISSION.....	10
4.12	ELECTRONIC TRANSMISSION (E-MAIL, FILE TRANSFER PROTOCOL, ETC.)	11
5	POLICY MAINTENANCE RESPONSIBILITY	11
6	POLICY EXCEPTIONS	11
7	POLICY REVIEW CYCLE.....	11
8	POLICY REFERENCES	11

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

1 Policy Definitions

- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Critical Systems:** Any system or application that is federally mandated/regulated, deemed critical by the data or system owner(s), or deemed a “24 hours, 7 days a week, 365 days a year” (24x7x365) application, will be defined as a critical system. CHFS ITMP will be the source of knowledge and repository of severity level for systems/applications.
- **Electronic Media:** includes but is not limited to, physical electronic media used to store information (ex. diskettes, magnetic tapes, desktops, laptops, hard drives, read only memory, compact disks, thumb drives, mobile devices, tablets, etc.). Laptops and mobile devices will be configured by COT Desktop Support to ensure the maximum level of security necessary to protect any sensitive data downloaded to that drive.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual’s tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person’s tax liability or potential tax liability.
- **Non-Electronic Media:** includes but is not limited to, hard copy or physical representation of information (ex. paper copies, printouts, drums, microfilm, handwritten notes, etc.).
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual’s identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual’s personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother’s maiden name, etc.).

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through a data media and security policy. This document establishes the agency's Data/Media Security Policy to manage risks and provide guidelines for security best practices regarding protecting the agency's data/media.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Advisor have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with organizations and/or agencies with the cabinet, which access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section [8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

4 Policy Requirements

4.1 General

All data and media must be sufficiently protected and monitored, consistent with CHFS IT policies and procedures, to prevent unauthorized use, modification, disclosure, destruction, and denial of service.

OATS IS Team and Enterprise documentation must apply security controls in a manner that is consistent with the value and classification of the data, as defined by NIST. Access to data/media is assigned on the “Principal of Least Privilege”, to users accessing only the information necessary to perform their job function(s). Access to data/media shall be subject to approval by appropriate management personnel. This policy shall align with all Commonwealth Office of Technology (COT) enterprise IT policies that pertain to data/media security.

4.2 Data Classification

The Information Technology Management Portal (ITMP) houses the criticality level of all CHFS applications. All CHFS applications will be reviewed by the owner of the data and reviewed by OATS IS Team to determine its level of criticality. If the environment has a mixed set of classified data, the classification that requires the most stringent controls must be applied. Any exception to this policy requires approval by OATS IS Team (see section 6 Policy Exceptions below).

4.3 External Markings

All sensitive data/media shall contain external restrictive markings for easy identification as CHFS property. The restrictive markings, including destruction and retention instructions are affixed to all media output to warn users of the degree of protection needed. Media belonging to external vendors, in the possession of CHFS employee/contractors, is subject to the same restrictive markings.

When a request for an external hard drive is granted the hard drive shall come to OATS for cataloging and proper labeling before being delivered to the employee.

4.4 External Storage Device Acquisition and Process

External storage via a cloud stage must follow the process steps outlined within the Enterprise IT Process: COT-078 COT Cloud Stage Gate Process. Any external hard drives that are approved, through the allocations process, shall be fully encrypted using a centrally managed encryption process managed by COT.

To request an external drive a submission must be made that includes a description of the business need and justification. The request shall be submitted to OATS for review and then forwarded to COT for further processing if approved. Before receiving a requested external hard drive the employee must complete the following:

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

- Education on the care and stewardship of keeping data secure and the standards for keeping an access/chain of custody log for any external storage utilized by an employee.
- A CHFS Employee Privacy and Security of Protected Health, Confidential, and Sensitive Information Agreement Form (CHFS-219) is to be signed by the employee receiving the external storage device outlining their responsibilities for the care and stewardship of the drive and confirmation of understanding their duties and any potential penalties for neglecting those duties.

4.5 Reproduction

When sensitive cabinet and/or agency data/media is reproduced in total or in part, the reproductions shall bear the same restrictive markings as the original.

Reproductions of sensitive data/media shall be kept to the minimum number of copies required. All CHFS employees and contractors are responsible to ensure that any sensitive information that is printed to a shared printer is picked up immediately and stored securely.

4.6 Storage and Security for Non-Electronic Media

All sensitive and confidential data/media entering or leaving offices, processing areas, or storage facilities must be appropriately secured, such that only authorized access is permitted. Storage solutions such as filing cabinets and/or drawers used for sensitive data/media shall be secured by a lock. Sensitive data must be placed behind two barriers of security while being stored. Please refer to the Internal Revenue Services (IRS) Publication 1075 for appropriate safeguards for Federal Tax Information (FTI) data.

4.7 Storage and Security for Electronic Media

All sensitive and confidential data/media entering or leaving offices, processing areas, or storage facilities must be appropriately secured, such that only authorized access is permitted.

As defined by COT Enterprise IT: CIO-072 Identity and Access Management Policy and CIO-092 Media Protection Policy all data/media must be securely stored and protected.

At no time shall any personal removable storage devices, devices not issued by the Commonwealth of Kentucky (Commonwealth), be attached to state owned workstations with the purpose of storing and/or retrieving electronic data/media. Computers are recommended to be secured by a cable lock when inside the building. All external storage devices shall be blocked unless it is a white listed device issued by the Commonwealth. This includes cell phones, flash drives (thumb drives), external CD/DVD burners, and any other form of external storage that is not a state issued external drive. Write to CD/DVD privileges shall be removed from the ability of employees unless a business need can be proven beyond a doubt.

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

CHFS reserves the right to perform unannounced audits/inspections to confirm that all external devices are being stored and secured properly per OATS guidelines, has the correct labeling and serial number for that device, a proper log of access/chain of custody to the drive has been kept, and that the employee does indeed still have the device. The employee shall produce, on demand the hard drive requested for inspection by OATS at the exact date and time it is requested, without warning or scheduling.

4.8 Disposal/Destruction for Non-Electronic Media

No sensitive information shall be disposed of by any publically accessible means. Sensitive information shall be afforded special handling regarding its disposal/destruction. This may include the use of shredders and/or special burn facilities including approved vendor services contracted by the Commonwealth.

4.9 Disposal/destruction for Electronic Media

All sensitive information on electronic media shall be properly disposed of in accordance with COT Enterprise IT: CIO-092 Media Protection Policy. All external drives being disposed of shall come through OATS for processing to remove the drive from the list of inventoried storage devices. The OATS agency/division will be responsible for forwarding the drive to COT for completion of the disposal process.

4.10 Shipping and Manual Handling

CHFS data/media shall not be supplied to vendors, contractors or other external organizations without properly executed contracts, agreements, (i.e. MOU, BAA, MOA, etc.), and confidentiality agreements. Contracts and agreements shall specify conditions of use, security requirements, and return dates. When shipping sensitive information, receipt of delivery must be verified, unless otherwise action/receipt is required by law or statutory regulation.

4.11 Facsimile Transmission

The OATS IS Team highly recommends that sensitive data never be transmitted via fax. If sensitive data must be transmitted via fax the following safeguards must be followed:

- The fax machine is located in a secure location so unauthorized individuals are not able to see sent/received information
- The recipient must be first notified when the fax will be transmitted. The recipient must agree that they, or an authorized person, will be at the device to collect the faxed data. Should no authorized person be present, the device must be in a secured state, so unauthorized persons may not have access to the faxed data.
- Always use a coversheet that includes the senders contact information and a confidentiality statement as defined and approved by each agency's management
- Do not include any sensitive information on the coversheet
- Confirm validity the recipient number before sending
- Sensitive CHFS data must not be faxed via non-trusted intermediaries such as, hotel staff, rented mailbox store staff, etc.

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

- If a fax is sent to, or received by, an incorrect recipient, immediately notify the OATS IS team at CHFSOATSSecurity@ky.gov

Following these precautions does not eliminate the risk of faxing. Please note that faxing over a non-secure/non encrypted line can easily be intercepted.

4.12 Electronic Transmission (E-mail, File Transfer Protocol, etc.)

When sensitive data is sent via the Internet or other unsecured media transmission facility, the data must be sent securely via one of the Commonwealth's approved methods (i.e. encryption, SSL, TLS, etc.) as defined by COT Enterprise IT: [CIO-091 Enterprise Information Security Program](#) and COT [Enterprise IT Process: COT-078 COT Cloud Stage Gate Process](#).

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in [CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy](#).

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- [Centers for Medicare and Medicaid Services \(CMS\) MARS-E 2.0](#)
- [CHFS Employee Privacy and Security of Protected Health, Confidential, and Sensitive Information Agreement Form \(CHFS-219\) CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy](#)
- [Enterprise IT Policy: CIO-072- Identity and Access Management Policy](#)
- [Enterprise IT Policy: CIO- 091- Enterprise Information Security Program Policy](#)
- [Enterprise IT Policy: CIO-092- Media Protection Policy](#)
- [Enterprise IT Process: COT-078 COT Cloud Stage Gate Process](#)
- [Internal Revenue Services \(IRS\) Publication 1075](#)
- [Information Technology Management Portal \(ITMP\)](#)

010.102 Data/Media Security Policy	Current Version: 2.4
010.000 Logical Security	Review Date: 11/15/2018

- Kentucky Revised Statute (KRS) Chapter 61.878- Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- Kentucky Revised Statute (KRS) Chapter 434.855- Misuse of computer information
- Kentucky Revised Statute (KRS) Chapter 514.030- Theft by unlawful taking or disposition
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information